

09/844,693

JUL 05 2007

REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is made obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-6, 8-23, 25-40 AND 42-51 UNDER 35 U.S.C. §103

Claims 1-6, 8-23, 25-40 and 42-51 stand rejected as being unpatentable over the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots") in view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya"). Although the Applicants disagree with the rejection, the Applicants have nevertheless amended independent claims 1, 18 and 35, from which claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 depend, in order to more clearly recite aspects of the present invention.

Particularly, the Examiner's attention is directed to the fact that Bots fails to disclose or suggest the novel invention of a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes (different from the master nodes), as well as facilitate VPN communications between the member nodes, and in which all communications between the member nodes are encrypted by the member nodes, as claimed in Applicants' amended independent claims 1, 18 and 35.

As the Applicants have previously argued, Bots at most teaches a security device (*i.e.*, a VPN unit or VPNU) that performs encryption or decryption on intercepted communications en-route between member nodes of VPNs. That is, as described by Bots at column 6, lines 37-52, the VPNU associated with a sender "will process the data packet from the sending side in such as way as to ensure that it [is] encrypted, authenticated and optionally compressed" (emphasis added). The VPNU associated with the receiver handles "the process of decrypting and authenticating the packets before forwarding it toward the destination endstation" (emphasis added). Thus, communications are encrypted as they travel between VPNUs, but not encrypted as they travel to/from nodes that are not VPNUs (*i.e.*, the sending node and the receiving

09/844,693

node).

The Examiner alleges, however, that Bots does teach encryption of all communication between member nodes, in order to "insure [sic] secure data communication between members of the same VPN group" (See, Office Action, Page 8). In support of this allegation, the Examiner cites to Bots at column 2, lines 55-62. The Applicants submit, however, that not only does this passage not teach that communications between member nodes of a VPN are encrypted, but that the passage also does not teach that these communications are encrypted by the member nodes. For example, reading on in the sentence that the Examiner quotes, it is stated that the secure data communications are ensured by "a site protector or VPN unit [that] implements a combination of techniques for data packet handling" (See, Bots at column 2, lines 56-58, emphasis added). Bots goes on to specify that these packet handling techniques include "compression, encryption and authentication" (See, Bots at column 2, lines 59-61). Thus, it is clear, as stated above, that encryption of communications in Bots is not performed by the member nodes of the VPN, as claimed by the Applicants, but by an intermediary (i.e., the VPNU). Moreover, it is clear that if the VPNU is performing the encryption and decryption, that the communications will only be encrypted as they travel from one VPNU to another VPNU, as the member nodes themselves are incapable of performing encryption and decryption. Thus, direct encrypted communications between member nodes are not possible.

Notably, Applicants' invention positively claims master nodes that control admission and departure in a VPN for an associated non-empty subset of member nodes (different from the master nodes), as well as facilitate VPN communications between the member nodes, and in which all communications between the member nodes are encrypted by the member nodes, as claimed in Applicants' amended independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35, as amended, positively recite:

1. A group management system comprising:
a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications

09/844,693

between said interconnected nodes are encrypted by said interconnected nodes; and
a plurality of master nodes, different from the plurality of interconnected nodes,
each of the master nodes controlling admission and departure in the VPN for an
associated non-empty subset of the member nodes and further facilitating said
communications between said plurality of interconnected nodes, wherein in the event
one of the master nodes fails, the associated subset of member nodes will be
automatically reassigned to one or more other of the master nodes. (Emphasis added)

18. A method for managing a group, the method comprising:
providing a plurality of interconnected nodes communicatively coupled with each
other as member nodes of a virtual private network ("VPN"), wherein all
communications between said interconnected nodes are encrypted by said
interconnected nodes; and
providing a plurality of master nodes, different from the plurality of interconnected
nodes, each of the master nodes controlling admission and departure in the VPN for an
associated non-empty subset of the member nodes and further facilitating said
communications between said plurality of interconnected nodes, wherein in the event
one of the master nodes fails, the associated subset of member nodes will be
automatically reassigned to one or more other of the master nodes. (Emphasis added)

35. A computer readable medium containing an executable program for managing a
group, where the program performs the steps of:
providing a plurality of interconnected nodes communicatively coupled with each
other as member nodes of a virtual private network ("VPN"), wherein all
communications between said interconnected nodes are encrypted by said
interconnected nodes; and
providing a plurality of master nodes, different from the plurality of interconnected
nodes, each of the master nodes controlling admission and departure in the VPN for an
associated non-empty subset of the member nodes and further facilitating said
communications between said plurality of interconnected nodes, wherein in the event
one of the master nodes fails, the associated subset of member nodes will be
automatically reassigned to one or more other of the master nodes. (Emphasis added)

The Applicants' invention is directed to systems and methods for scalable
distributed management of virtual private networks (VPNs). The management of
encrypted group communications necessary to establish secure, private VPN
communications channels through an underlying public network infrastructure places a
variety of burdens on a VPN manager. In particular, the addition or removal of a
member from a VPN often involves the generation and distribution of one or more new
encryption keys that allow current VPN members to decrypt private communications

09/844,693

sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN, which communicate directly with each other via encrypted communications, into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (i.e., admission and departure) in the VPN and to facilitate VPN communications for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and management burdens are not placed entirely on a single master node. This eliminates the single point of failure, because if one master node fails, any one of a plurality of other master nodes is available to assume the failed node's responsibilities. Moreover, the member nodes are able to use the distributed encryption keys to communicate directly with each other using encrypted communications. Thus, a VPN employing such an architecture is more easily scalable than a VPN employing a more conventional architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node.

The Applicants' invention positively claims that communications between member nodes (different from master nodes) are encrypted by the member nodes. That is, in at least claims 1, 18 and 35, the Applicants recite the limitation of encrypted communications by and between member nodes of a VPN. As described above, Bots does not teach or suggest a mechanism for allowing direct, encrypted communications between member nodes, but rather teaches a communication intercept point that encrypts or decrypts messages seen by the nodes as ordinary Internet data packet transfers.

RECEIVED
CENTRAL FAX CENTER**JUL 05 2007**

09/844,693

Bots thus fails to teach or anticipate a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes (different from the master nodes), and in which all communications between the member nodes are encrypted by the member nodes, as positively claimed by the Applicants in amended claims 1, 18 and 35. Pandya fails to bridge this gap in the teachings of Bots. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35, as amended, fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 are not made obvious by the teachings of Bots in view of Pandya. Therefore, the Applicants submit that dependent claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

II. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.


If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

09/844,693

Respectfully submitted,

7/5/07
Date

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702


Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404